PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s) : Kamperman et al.   Examiner: Richard G. Keehn

Serial No.   : 10/565,663   Group Art Unit: 2456

Filed   : January 23, 2006   Confirmation No.: 2420

For   : **USER HYBRID DEVICE AND PERSON BASED AUTHORIZED DOMAIN ARCHITECTURE**

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

  Appellants herewith respectfully present its Brief on Appeal as follows:

REAL PARTY IN INTEREST

The real party in interest is Koninklijke Philips Electronics N.V., a corporation of The Netherlands having an Office and a place of business at Groenewoudseweg 1, Eindhoven, Netherlands 5621 BA. Koninklijke Philips Electronics N.V. is the parent company of the assignee of record U.S. Philips Corporation, a Delaware corporation having an Office and a place of business at 345 Scarborough Road, Briarcliff Manor, New York, 10510-8001.

RELATED APPEALS AND INTERFERENCES

To the best of Appellants' knowledge and belief, there are no currently pending related appeals, interferences or judicial proceedings.

STATUS OF CLAIMS

Claims *1, 3, 4, 6-12, 14, 15 and 17-23* are pending in this application. In the Final Office Action that mailed March 25, 2010, Claims *1, 3, 4, 6-12, 14, 15 and 17-23* stand rejected. In the Advisory Action that mailed November 3, 2010, the Office maintains the rejections of Claims *1, 3, 4, 6-12, 14, 15 and 17-23*.

STATUS OF AMENDMENTS

In an Amendment filed October 27, 2010, in response to the Final office Action mailed August 27, 2010, Claims *1, 3, 4, 6-12, 14, 15 and 17-23* remain pending, with Claims 1 and 12 being in independent form. This Appeal Brief is in response to the Final office Action that rejected Claims *1, 3, 4, 6-12, 14, 15 and 17-23* and the Advisory Action mailed on November 3, 2010 that maintained the rejection of Claims *1, 3, 4, 6-12, 14, 15 and 17-23*.

SUMMARY OF CLAIMED SUBJECT MATTER

The claimed subject matter relates to a system and method of generating an Authorized Domain.

The concept of Authorized Domains (ADs) tries to find a solution to both serve the interests of the content owners (that want protection of their copyrights) and the content consumers (that want unrestricted use of the content). The basic principle is to have a controlled network environment in which content can be used relatively freely as long as it does not cross the border of the authorized domain. Typically, authorized domains are centered around the home environment, also referred to as home networks. Of course, other scenarios are also possible. A user could for example take a portable device for audio and/or video with a limited amount of content with him on a trip, and use it in his hotel room to access or download additional content stored on his personal audio and/or video system at home. Even though the portable device is outside the home network, it is a part of the user's authorized domain. In this way, an Authorized Domain (AD) is a system that allows access to content by devices in the domain, but not by any others.

Prior art solutions of Authorized Domains are of two types, device based Authorized Domains (ADs) and person based Authorized Domains. In typical device based ADs, the domain is formed by a specific set of devices and content. Only the specific set of devices of the domain is allowed to access, use, etc. the content of that domain. There is no distinction of the various users of the specific set of devices. A drawback of device based AD systems is that they typically do not provide the typical flexibility that a user wants or need, since users are restricted to a particular and limited set of devices. In this way, a user is not allowed to exercise the rights that the user has obtained anytime and anywhere he chooses. For example, if a user is visiting a friend's house he is not able to access his legally purchased content on the friend's devices as these devices would not typically be part of the particular and limited set of devices forming the

domain comprising the user's content.

In a user based Authorized Domain, where the domain is based on persons instead of devices, access to content bound to an AD is allowed by only a specific and limited set of users using any compliant device. Person based Authorized Domains typically offer easier domain management compared to device based ADs. However, person based systems require person identification which is not always convenient or preferred by users. Further, a visitor to your home may want to access your content. As he does not have a person id device for that domain it is not possible for him to access content. It would be preferred if devices in the home belonging to the domain could enable access of domain content by the visitor.

The present invention overcomes these obstacles by claiming **a hybrid person and device based authorized domain** having the individual advantages of each system. Accordingly, the present invention provides a method and corresponding system for providing an Authorized Domain structure based on both persons and devices. More particularly, the claimed subject matter relates to a system and a method of generating an Authorized Domain (AD) by selecting a domain identifier, and binding at least one user (P1, P, PN1), at least one device (D1, D2, . . . , DM), and at least one content item (C1, C2, . . . , CNZ) to the Authorized Domain (AD) given by the domain identifier (Domain ID). Hereby, a number of verified devices (D1, D2, . . . , DM) and a number of verified persons (P1, P2, . . . , PN1) that is authorized to access a content item of said Authorized Domain (100) is obtained. In this manner, access to a content item of an authorized domain by a user operating a device is obtained either by verifying that **the content item and the user** is linked to the same domain or by verifying that **the device and the content item** is linked to the same domain. Thereby, enhanced flexibility for one or more users when accessing content in an authorized domain is obtained while security of the content is still maintained.

Independent Claim 1

The subject matter, as recited in independent claim 1, relates to a method of generating an Authorized Domain (AD), the method comprising:

> selecting a domain identifier (Domain_ID) uniquely identifying the Authorized Domain (AD),
>
> binding at least one user $(P1, P2, ..., PN_1)$ to the domain identifier (Domain_ID),
>
> binding at least one device $(D1, D2, ..., DM)$ to the domain identifier (Domain_ID), and
>
> binding at least one content item $(C1, C2, ..., CN_2)$ to the Authorized Domain (AD) given by the domain identifier (Domain_ID),
>
> thereby obtaining a number of devices $(D1, D2, ..., DM)$ and a number of users $(P1, P2, ..., PN_1)$

that are authorized to access content items $(C1, C2, ..., CN_2)$ of said Authorized Domain (AD)

> wherein access to the at least one content item $(C1, C2, ..., CN_2)$ is obtained, via an authorization

certificate, by verifying that the at least one content item $(C1, C2, ..., CN_2)$ and the at least one user $(P1, P2, ..., PN_1)$ are linked to the same domain identifier (Domain_ID) or by verifying that the at least one device $(D1, D2, ..., DM)$ and the at least one content item $(C1, C2, ..., CN_2)$) are linked to the same domain identifier (Domain_ID);

> wherein the authorization certificate includes the domain identifier (Domain_ID) as a holder of the

authorization certificate.

Independent Claim 12

The subject matter, as recited in independent claim 12, relates to a system for generating an Authorized Domain (AD), the system comprising:

> means for obtaining a domain identifier (Domain_ID) uniquely identifying the Authorized Domain (AD),
>
> means for binding at least one user $(P1, P2, ..., PN_1)$ to the domain identifier (Domain_ID),
>
> means for binding at least one device $(D1, D2, ..., DM)$ to the domain identifier (Domain_ID), and
>
> means for binding at least one content item $(C1, C2, ..., CN_2)$ to the Authorized Domain (AD) given by the domain identifier (Domain_ID),
>
> thereby obtaining a number of devices $(D1, D2, ..., DM)$ and a number of users $(P1, P2, ..., PN_1)$

that is authorized to access content items $(C1, C2, ..., CN_2)$ of said Authorized Domain (AD)

wherein access to the at least one content item (C1, C2, ..., CN_2) is obtained, via an authorization certificate, by verifying that the at least one content item (C1, C2, ..., CN_2) and the at least one user (P1, P2, ..., PN_1) are linked to the same domain identifier (Domain_ID) or by verifying that the at least one device (D1, D2, ..., DM) and the at least one content item (C1, C2, ..., CN_2) are linked to the same domain identifier (Domain_ID);

wherein the authorization certificate includes the domain identifier (Domain_ID) as a holder of the authorization certificate.

Support in the published specification (2006/0190621) for claims *1, 3, 4, 6-12, 14, 15 and 17-23* can be found as follows:

Claim 1 (*See* Abstract, par. 16);

Claim 2 (Cancelled);

Claim 3 (*See* par. 18);

Claim 4 (*See* par. 20);

Claim 5 (Cancelled);

Claim 6 (*See* par. 25);

Claim 7 (*See* par. 26);

Claim 8 (*See* par. 31-35);

Claim 9 (*See* par. 36);

Claim 10 (*See* par. 38);

Claim 11 (*See* par. 39);

Claim 12 (*See* Abstract, par. 16);

Claim 13 (Cancelled);

Claim 14 (*See* par. 16, 18);

Claim 15 (*See* par. 25, 26);

Claim 16 (Cancelled);

Claim 17 (See par. 13);

Claim 18 (*See* par. 26);

Claim 19 (*See* par. 87, 88, 95);

Claim 20 (*See* par. 36);

Claim 21 (*See* par. 38);

Claim 22 (*See* par. 78);

Claim 23 (*See* par. 1, 46);

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection to be reviewed are:

(1)   Whether independent claims 1 and 12 are unpatentable under 35 U.S.C.
§103(a) over U.S. Patent Publication No. 2003/0018491 ("Nakahara") and further in view of
U.S. Patent No. 6,324,645 ("Andrews").

The Appellants respectfully request the Board to address the patentability of independent
claims 1 and 12. This position is provided for the specific purpose and stated purpose of
simplifying the current issue on appeal. However, the Appellants herein specifically reserve the
right to argue and address the patentability of each of the further claims at a later date should the
separately patentable subject matter of those claims at a later date should the separately
patentable subject matter of those claims later become an issue. Accordingly, this limitation of
the subject matter presented for appeal herein, specifically limited to discussions of the
patentability of claims 1 and 12 is not intended as a waiver of Appellants' right to argue the
patentability of the further claims and claim elements at that later time.

I. ARGUMENT

The Examiner's position

Independent Claims 1 and 12

In the Final Office Action, mail date, August 27, 2010, with regard to independent claims 1 and 12, the Examiner states, at page 4, that Nakahara discloses and a system for generating an Authorized Domain (AD), comprising:

- selecting a domain identifier (Domain_ID) uniquely identifying the Authorized Domain (AD). **See Nakahara pages 12-13, par. 200.**

- binding at least one user (P1, P2, ..., PN_1) to the domain identifier (Domain_ID), **See Nakahara page 13, par. 197 and 200.**

- binding at least one device (D1, D2, ..., DM) to the domain identifier (Domain_ID), and **See Nakahara page 13, par. 200.**

- binding at least one content item (C1, C2, ..., CN_2) to the Authorized Domain (AD) given by the domain identifier (Domain_ID), **See Nakahara pages 13, par. 200.**

- thereby obtaining a number of devices (D1, D2, ..., DM) and a number of users (P1, P2, ..., PN_1) that are authorized to access content items (C1, C2, ..., CN_2) of said Authorized Domain (AD) **See Nakahara pages 12-13, par. 200.**

- wherein access to the at least one content item (C1, C2, ..., CN_2) is obtained, via an authorization certificate, by verifying that the at least one content item (C1, C2, ..., CN_2) and the at least one user (P1, P2, ..., PN_1) are linked to the same domain identifier (Domain_ID) or by verifying that the at least one device (D1, D2, ..., DM) and the at least one content item (C1, C2, ..., CN_2)) are linked to the same domain identifier (Domain_ID); **See Nakahara page 12, par. 197, via an authorized certificate, page 12, par. 198.**

- wherein the authorization certificate includes the domain identifier (Domain_ID) as a holder of the authorization certificate. **See Nakahara page 12, par. 198.**

The Examiner admits that Nakahara does not explicitly disclose – including the domain identifier as a holder of the authorized certificate.. The Examiner relies on Andrews for curing the deficiency in Nakahara. More particularly, the Examiner cites Andrews at col. 9, lines 49-58 for disclosing - *inclusion of the domain id as a holder of the authorized certificate.*

The Advisory Action

In the Advisory Action, mail date November 3, 2010, the Examiner states that Applicant argues that Nakahara is directed exclusively to device based domains and not a hybrid user/device domain. The Examiner must examine what is in the claims. The Examiner asserts that the claims make no mention, either implicitly or explicitly of hybrid user/device based domains. The claims recite, inter alia, "binding at least one user (P1, P2,…..PN1) to the domain identifier". Binding to the domain identifier does not make a hybrid user/device domain, but merely associates a user to a domain, just as Nakahara does. The Examiner goes on to state that, there are countless places in Nakahara, in addition to those passages cited in the previous Office action where a user is bound to a domain, for instance, par. 198.

The Applicant argues that Nakahara does not disclose users as identifiers included in data structures, represented as elements of the domain structure. But this is not claimed. Applicant's claims recited binding at least one user, not that a user is an identifier, nor that a user is an element of the domain structure. Therefore, Applicant argues that which is not claimed. Applicants remaining arguments, based on the assertions on page 11, are not persuasive for the same reasons.

The Appellant's position

(A)   The combination of Nakahara and Andrews Medvinsky does not make obvious the invention of independent claims 1 and 12.

Appellants contend that each of these claims, and in particular independent claims 1 and 12, are patentably distinct from teachings of Nakahara and Andrews, taken alone or in any proper combination. Accordingly, Appellants hereby respectfully present to the Board the following arguments in support of their position that Claims 1 and 12 are patentably distinct over the teachings of Nakahara and Andrews, taken alone or in any proper combination.

As set forth in MPEP §2143, a *prima facia* case of obviousness requires that "prior art reference(s) must teach or suggest all of the claim limitations." *See, e.g., In re Royka*, 180 USPQ 580 (CCPA 1974).

Regarding the rejection of claims 1 and 12, Appellants respectfully submit that Nakahara is directed **exclusively to device based domains** and not to hybrid user/device based domains, as disclosed by the present invention. In Nakahara, users appear to only play a role as owners of such a domain, but are not represented, for example, as identifiers included in data structures, represented as elements of the domain structure. Accordingly, it is respectfully submitted that Nakahara does not teach or suggest at least the step of:

binding at least one user (P1, P2, …, PN$_1$) to the domain identifier (Domain_ID),

In the Office Action, it is suggested that Nakahara discloses "Searcher X" **belonging to the domain**. The Office cites Nakahara at page 13, par. 197 and 200 in support. Applicants respectfully disagree. It is respectfully submitted that "Searcher X" is not identified/defined as a user, nor is "Searcher X" identified as a member of the domain. This is shown in Nakahara, at pars. 172 and 174. Specifically, par. 174 states in relevant part, *"when the searcher X is any of*

the license management units" and par. 172 states in relevant part, "*content output units*". Both

citations suggest that "Searcher X" is not intended to be identified/defined as a user or identified

as a member of the domain. Instead, Nakahara is merely teaching that the "Searcher X" is a

pseudonym for a kind of role that a device/unit may have, <u>but not a user</u>.

Claim 1 further requires in part:

"*binding at least one content item (C1, C2, ..., CN₂) to the Authorized Domain (AD)*
given by the domain identifier (Domain_ID)"

It is respectfully submitted that Nakahara does not teach the above claim element

pertaining to binding at least one content item. In the Office Action it is suggested that

Nakahara discloses the content usage devices belonging to the domain at page 13, par. 200. It

is respectfully submitted that "content usage **devices**" are entirely different from "content

items".

With continued reference to claim 1, this claim further requires in part:

"*thereby obtaining a number of devices (D1, D2, ..., DM) and a number of users (P1, P2,*
..., PN₁) that are authorized to access content items (C1, C2, ..., CN₂) of said Authorized
Domain (AD)"

It is respectfully submitted that Nakahara does not teach the above claim element. In

the Office Action it is suggested that Nakahara discloses the domain list {Domain ID}, at

least one user {user}, function units {devices}, and content usage devices {content items},

and licensing {authorized} at pages 12-13, par. 200. As previously discussed above,

Nakahara does not disclose at least one user or content items belonging to the domain. It

therefore follows that Nakahara does not disclose at least one user and/or content item being

disclosed in the domain list.

With continued reference to claim 1, this claim further requires in part:

"*wherein access to the at least one content item (C1, C2, ..., CN$_2$) is obtained, via an authorization certificate, by verifying that the at least one content item (C1, C2, ..., CN$_2$) and the at least one user (P1, P2, ..., PN$_1$) are linked to the same domain identifier (Domain_ID) or by verifying that the at least one device (D1, D2, ..., DM) and the at least one content item (C1, C2, ..., CN$_2$)) are linked to the same domain identifier (Domain_ID)*"

It is respectfully submitted that Nakahara does not teach the above claim element. In the Office Action it is suggested that Nakahara discloses granting or restricting access to content based on whether the user and content domain licensing requirements are met – page 12, see par. 197, via an authorized certificate, see par. 198. However, par. 198 of Nakahara clearly states that the certificate is purely a regular identity certificate used to identify a component, which is different from a domain related certificate. Accordingly, the certificate of Nakahara should not be considered an authorized certificate related to a domain.

In the Final Office Action, the Examiner admits that Nakahara does not explicitly disclose – including the domain identifier as a holder of the authorized certificate.. The Examiner relies on Andrews for curing the deficiency in Nakahara. More particularly, the Examiner cites Andrews at col. 9, lines 49-58 for disclosing - *inclusion of the domain id as a holder of the authorized certificate.* According to the invention, a certificate creates or defines part of the domain, while in Andrews, it refers to members of the domain. In further contrast, the types of domains referred to in Andrews is a privilege/administrative domain, while the invention refers to content-access domains.

It is instructive to explain, by way of illustration, how the present invention binds persons, devices, user rights and contents in an authorized domain (AD) in a manner neither taught nor suggested by the cited and applied art. FIG. 1 of Appellant's specification, schematically

Atty. Docket No. Appeal Brief - NL040388US2 [MS-470]

illustrates binding of persons, devices, user rights and content in an authorized domain (AD).
Shown is an authorized domain (100) according to the present invention where a number of
devices D1, D2, D3, . . . , DM (where M is equal to or larger than 1), a number of content items
C1, C2, C3, . . . , CN.sub.2 (where N.sub.2 is equal to or larger than 1) and a number of
persons/users P1, P2, P3, . . . , PN.sub.1 (where N.sub.1 is equal to or larger than 1) is bound to
the AD according to an embodiment of the present invention.

The devices, persons, and content items have been bound to the domain (100). Also shown
are one or more user rights (URC1, . . . URCN.sub.2), where preferably one content item is
associated with one user right certificate specifying which rights a given person (or alternatively
a given group of persons and/or all persons bound to the domain (100)) have in relation to the
specific content item (or alternatively, several or all content items in the domain (100)).

DEFINITIONS:

(1) **Content (C1, C2, C3, . . . , CN.sub.2):** content items are preferably encrypted
(there are many options, for example with a unique key per content title) and can
be anywhere in the system; a content item is in this embodiment linked indirectly
to a user right certificate via a content right, as also explained in connection with
FIG. 4a.

(2) **Content right (CR; not shown; see e.g. FIG. 4a):** contains cryptographic key(s)
or other suitable protection means to access a certain (encrypted/protected) content
item. The system is flexible in the sense that content rights can be made unique per
content title or even unique per specimen (copy) of content. Content rights should
be only transferred to compliant devices. A more secure rule is to enforce that
content rights may be only transferred to compliant devices that are operated by
authorized users (i.e. users that are authorized to have access to the specific content
right by means of their user rights). Content rights might also be stored together

with the content on for example an optical disk. However, content rights must be
stored securely since they contain the content decryption key.

(3) **User right certificate (URC1, . . . URCN.sub.2):** a certificate or the like issued
by the content provider that authorizes a person to use a certain content right (CR)
(belonging to a certain piece of content). User rights can be in principle anywhere
in the system. Preferably, the user right certificate also comprises rules (e.g.
restricted to viewers 18 years or older, or European market only, etc.) of access to a
certain content item.   The user right (URC1, . . . URCN.sub.2) is a single
connection, binding, coupling etc. **between one user and a content right** (which
is required to decrypt a piece of content).

(4) **Device (D1, D2, D3, . . . , DM):** a device that is used to play, operate, record,
present, display, modify, etc. a content item. Additionally, a (compliant) device can
also preferably identify a user by means of a personalized identification device
(e.g. such as a smart-card, a mobile phone, a biometric sensor, etc.) and collect
certificates (e.g. from the smartcard, or from other devices) that prove that the user
is allowed to use a certain content right This content right could be obtained from
the smart-card where it was stored (if it was stored there), or be obtained (securely
transferred) from another compliant device on a network.

(5) **User person (P1, P2, P3, . . . , PN.sub.1):** A user is identified by some biometric
or preferably by a personalized identification device (e.g. a smartcard, mobile
phone, a mobile phone containing a smartcard or other types of devices that
uniquely identifies a user) that he/she is wearing, carrying or has access to. A
mobile phone comprising a smart card or another device having storage means is
preferred since it allows users to carry rights with them (for accessing content on
off-line devices). The identification device may itself be protected by a biometric
authentication mechanism, so that anyone other than the legitimate owner cannot

use the identification device. A user may also be identified using public key technology or zero-knowledge protocols or a combination thereof.

Preferably, authorized devices are bound to the AD (100) by a certificate. Likewise authorized persons/users are preferably also bound to the AD (100) via certificates. In one embodiment, Content items are bound to a person (user) by means of a user right certificate (URC). This user right certificate (URC) enables the use of a corresponding content right (CR) that preferably contains a cryptographic key for accessing the content. As described above, a user right certificate (URC) is typically linked with one content item, but could also be linked with multiple content items. An exemplary partial data structure of a content container (contains a content item), a URC and a CR are shown and explained in greater detail in connection with FIG. 4a.

In the example shown in FIG. 1, each content item C1, C2, . . . , CN2 is coupled to a user right certificate URC1, URC2, . . . , URC N_2. URC1 and URC2 are coupled to person P1, URC3 coupled to person P2, URC_{2-2}, URC_{2-1} and URC_2 are coupled to person PN_1, and URC4-URC_{2-3} are distributed among person(s) P3-PN_{1-1}.

In this way,
- specific content C1 and C2 are coupled to a specific person P1, via URC1 & URC2
- specific content C3 coupled to a specific person P2, via URC3
- specific content CN_{2-2}, CN_{2-1} and CN_2 are coupled to a specific person PN_1, via , URC_{2-2}, URC_{2-1} and URC_2 and
- specific content C4-CN_{2-3} are distributed among specific person(s) P3-PN $_{1-1}$ via their respective URC.

In this shown embodiment, a single content item is only allowed to be coupled to a single

URC (indirectly via a content right) and thereby a single person. If several users needs a copy

of the same content item it would in this embodiment be present once for each user and treated

as different content items, which make rights management simpler. Alternatively and just as

applicable, a single content item could be coupled to more than one person, as a CR can be

linked to multiple URCs.

Persons P1, P2, . . . , PN$_1$ and Domain devices D1, D2, . . . , DM are then grouped into

forming the authorized domain (100). Preferably, the binding, i.e. grouping and coupling, of

devices, persons and content is according to the present invention done by the use of

certificates. Preferably a Domain Devices Certificate or Domain Devices List (DDC), a

Domain Users Certificate or Domain Users List (DUC), **and a User Right Certificate** or User

Right List (URC) are used. In the following reference is only made to certificates, although it is

to be understood that such structures may e.g. be implemented as lists or the like instead.

The DDC lists the device(s), which are part of the domain (100), e.g. by comprising for

each device a unique identifier. The DUC lists the user(s), which are part of the domain, e.g. by

comprising a unique identifier or a (e.g. public) cryptographic key or a hash thereof for each

user. In a preferred embodiment, the DDC and DUC are associated with each other by means

of a Domain Identifier (Domain_ID) contained in both certificates. **In this way, a very simple**

way of linking the user(s) (and thereby the content item(s)) and the device(s) of a given

domain together (and thereby forming the domain) is obtained.

In operation

If a specific device (e.g. device D3) wants to access a certain piece of content (e.g.

content C1) it has to be proved or checked, etc. (using the certificates) **that the certain piece**

of content is coupled to a specific person (e.g. person P1) that is a member of the same

domain (100) as the specific device. This may e.g. by done by checking that an (unique)

identifier of the specific device (e.g. device D3) is part of the DDC, that an (unique) identifier

of the specific person (e.g. person P1) is part of the DUC, **that both the DDC and DUC comprises the same Domain Identifier** (e.g. Domain_ID=4 or Domain_ID=8 byte value (e.g. generated randomly); not shown), and that the URC for the specific person (e.g. URC1) specifies that the specific person has the right to access the certain piece of content (e.g. if it is within the validity period of his license or have not been used more than three times. By having the content items coupled to persons (via URCs) the ownership of content is easily reflected. Additionally, it is easier to administer a split of the AD, since by splitting the persons the appropriate content items is also split, since the content items are linked to persons.

Claim 1 recites in relevant part:

> wherein access to the at least one content item (C1, C2, ..., CN$_2$) is obtained, via an
> authorization certificate, by verifying that the at least one content item (C1, C2, ..., CN$_2$)
> and the at least one user (P1, P2, ..., PN$_1$) are linked to the same domain identifier
> (Domain_ID) or by verifying that the at least one device (D1, D2, ..., DM) and the at least
> one content item (C1, C2, ..., CN$_2$)) are linked to the same domain identifier
> (Domain_ID);

Hereby, one or more devices, one or more persons, and at least one content item (via a person) are linked together in the domain preferably with the use of certificates or alternatively with the use of lists comprising the same described elements as for the certificates. It may be possible for the domain to comprise zero persons and/or zero devices and/or zero content items during some points. E.g. when initially building the domain it may comprise zero content items or zero devices bound to the domain, etc. In this way, a user that has been verified as belonging to the same domain as the content item being accessed may access the specific content using any device. Additionally, a user that is using a device that has been verified as belonging to the same domain as the content item being accessed may access the specific content using that specific device. Further all users may access the specific content item on that specific device. This gives enhanced flexibility for one or more users when accessing content in
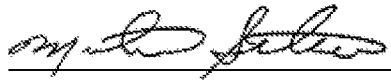
an ▨▨ while security of the content is still maintaining.

In view of at least the foregoing, Appellants submit that claims 1 and 12 are patentable over Nakahara and Andrews.

CONCLUSION

For at least the reasons stated above, all of the claims are submitted to be patentable. Reversal of the rejections by the Board is respectfully requested.

Respectfully submitted,

Michael A. Scaturro
Reg. No. 51,356
Attorney for Applicant

Mailing Address:
Intellectual Property Counsel
Philips Electronics North America Corp.
P.O. Box 3001
345 Scarborough Road
Briarcliff Manor, New York 10510-8001

CLAIMS APPENDIX

CLAIMS ON APPEAL

1. A method of generating an Authorized Domain (AD) comprises:

   selecting a domain identifier (Domain_ID) uniquely identifying the Authorized Domain (AD),

   binding at least one user (P1, P2, ..., PN_1) to the domain identifier (Domain_ID),

   binding at least one device (D1, D2, ..., DM) to the domain identifier (Domain_ID), and

   binding at least one content item (C1, C2, ..., CN_2) to the Authorized Domain (AD) given by the domain identifier (Domain_ID),

   thereby obtaining a number of devices (D1, D2, ..., DM) and a number of users (P1, P2, ..., PN_1) that are authorized to access content items (C1, C2, ..., CN_2) of said Authorized Domain (AD)

   wherein access to the at least one content item (C1, C2, ..., CN_2) is obtained, via an authorization certificate, by verifying that the at least one content item (C1, C2, ..., CN_2) and the at least one user (P1, P2, ..., PN_1) are linked to the same domain identifier (Domain_ID) or by verifying that the at least one device (D1, D2, ..., DM) and the at least one content item (C1, C2, ..., CN_2)) are linked to the same domain identifier (Domain_ID);

   wherein the authorization certificate includes the domain identifier (Domain_ID) as a holder of the authorization certificate.

2. (Cancelled)

Appl. No. 10/565,663   **Page 25 of 34**

Appeal Brief

3.   A method according to claim 1, wherein the binding at least one user (P1, P2, ..., PN_1) to the domain identifier (Domain_ID) comprises:

      obtaining or generating a Domain Users List (DUC) comprising the domain identifier (Domain_ID) and a unique identifier (Pers_ID1, Pers_ID2, ..., $Pers\_IDN_1$) for a user (P1, P2, ..., PN_1) thereby defining that the user is bound to the Authorized Domain (AD),

and/or in that

      the binding at least one device (D1, D2, ..., DM) to the domain identifier (Domain_ID)

comprises:

      obtaining or generating a Domain Devices List (DDC) comprising the domain identifier (Domain_ID) and a unique identifier (Dev.ID1, Dev.ID2, ..., Dev.IDM) for a device (D1, D2, ..., DM) thereby defining that the device is bound to the Authorized Domain (AD).

4. A method according to claim 3, wherein the binding at least one content item (C1, C2, ..., CN_2) to the Authorized Domain (AD) comprises:

      binding a content item (C1, C2, ..., CN_2) to a User Right (URC1, URC2, ... $URCN_2$), where said User Right (URC1, URC2, ... $URCN_2$) is bound to a user (P1, P2, ..., PN_1) which is bound to the Authorized Domain (AD), and/or

      binding a content item (C1, C2, ..., CN_2) to a Device Right (DevRC), where said Device Right (DevRC) is bound to a device (D1, D2, ..., DM) which is bound to the Authorized Domain (AD), and/or

      binding a content item (C1, C2, ..., CN_2) to a Domain Rights (DRC1, DRC2, ... $DRCN_2$), where said Domain Rights (DRC1, DRC2, ... $DRCN_2$) is bound to the Authorized Domain (AD).

5. (Cancelled)

6.   A method according to claim 4, wherein the User Right (URC1, URC2, ... $URCN_2$) or the Device Right (DevRC) or the Domain Rights (DRC1, DRC2, ... $DRCN_2$) comprises rights data (Rghts Dat) representing which rights exists in relation to the at least one content item (C1, C2,

Atty. Docket No. Appeal Brief - NL040388US2 [MS-470]

..., CN_2) bound to the User Right (URC1, URC2, ... $URCN_2$) or the Device Right (DevRC) or the Domain Rights (DRC1, DRC2, ... $DRCN_2$).

7. A method according to claim 1, the method further comprises controlling access to a given content item bound to the Authorized Domain (AD) by a given device being operated by a given user, comprising:

checking if the given user is bound to the same Authorized Domain (AD) as the given content item, or

checking if the given device is bound to the same Authorized Domain (AD) as the given content item,

and allowing access for the given user via the given device and/or other devices to the content item if the given user is bound to the same Authorized Domain (AD),

or allowing access for the given user and/or other users via the given device to the content item if the given device is part of the same Authorized Domain (AD).

8. A method according to claim 3, the method further comprises controlling access to a given content item (C1, C2, ..., CN_2), being bound to the Authorized Domain (AD) and having a unique content identifier (Cont_ID), by a given device being operated by a given user comprising:

checking if the Domain Devices List (DDC) of the Authorized Domain (AD) comprises an identifier (Dev.ID) of the given device, thereby checking if the given device is bound to the same Authorized Domain (AD) as the content item, and/or

checking if the Domain User List (DUC) of the Authorized Domain (AD) comprises an identifier (Pers_ID) of the given user (P1, P2, ..., PN_1) thereby checking if the given user is bound to the same Authorized Domain (AD) as the content item,

and allowing access to the given content item (C1, C2, ..., CN_2) by the given device (D1, D2, ..., DM) for any user if the given device is bound to the same Authorized Domain (AD) as the content item being accessed, and/or

allowing access to the given content item $(C1, C2, \ldots, CN_2)$ by any device including the given device for the given user if the given user is bound to the same Authorized Domain (AD) as the content item being accessed.

9. A method according to claim 7, wherein the binding at least one content item $(C1, C2, \ldots, CN_2)$ to the Authorized Domain (AD) comprises:

binding a content item $(C1, C2, \ldots, CN_2)$ to a User Right $(URC1, URC2, \ldots URCN_2)$, where said User Right $(URC1, URC2, \ldots URCN_2)$ is bound to a user $(P1, P2, \ldots, PN_1)$ which is bound to the Authorized Domain (AD), and

wherein the controlling access of a given content item further comprises:

checking that the User Right $(URC1, URC2, \ldots URCN_2)$ for the given content item specifies that the given user $(P1, P2, \ldots, PN_1)$ has a right to access the given content item $(C1, C2, \ldots, CN_2)$ and only allowing access to the given content item $(C1, C2, \ldots, CN_2)$ in the affirmative.

10. A method according to claim 1, wherein every content item is encrypted and that a content right (CR) is bound to each content item and to a User Right (URC) or a Device Right (DevRC) or a Domain Rights (DRC), and that the content right (CR) of a given content item comprises a decryption key for decrypting the given content item.

11. A method according to claim 4, wherein

the Domain Users List (DUC) is implemented as or included in a Domain Users Certificate, and/or

the Domain Devices List (DDC) is implemented as or included in a Domain Devices Certificate, and/or

the User Right $(URC1, URC2, \ldots, URCN_2)$ is implemented as or included in a User Right Certificate, and/or

the Device Right (DevRC) is implemented as or included in a Device Right Certificate, and/or

the Domain Rights (DRC1, DRC2, ..., DRCN$_2$) is implemented as or included in a

Domain Rights Certificate.

12. A system for generating an Authorized Domain (AD), the system comprising:

means for obtaining a domain identifier (Domain_ID) uniquely identifying the

Authorized Domain (AD),

means for binding at least one user (P1, P2, ..., PN$_1$) to the domain identifier

(Domain_ID),

means for binding at least one device (D1, D2, ..., DM) to the domain identifier

(Domain_ID), and

means for binding at least one content item (C1, C2, ..., CN$_2$) to the Authorized Domain

(AD) given by the domain identifier (Domain_ID),

thereby obtaining a number of devices (D1, D2, ..., DM) and a number of users (P1, P2,

..., PN$_1$) that is authorized to access content items (C1, C2, ..., CN$_2$) of said Authorized Domain

(AD)

wherein access to the at least one content item (C1, C2, ..., CN$_2$) is obtained, via an

authorization certificate, by verifying that the at least one content item (C1, C2, ..., CN$_2$) and the

at least one user (P1, P2, ..., PN$_1$) are linked to the same domain identifier (Domain_ID) or by

verifying that the at least one device (D1, D2, ..., DM) and the at least one content item (C1, C2,

..., CN$_2$) are linked to the same domain identifier (Domain_ID);

wherein the authorization certificate includes the domain identifier (Domain_ID) as a

holder of the authorization certificate.

13. (Cancelled)

14.   A system according to claim 12, wherein the means for binding at least one user (P1, P2, …, PN_1) to the domain identifier (Domain_ID) is adapted to

obtain or generate a Domain Users List (DUC) comprising the domain identifier (Domain_ID) and a unique identifier (Pers_ID1, Pers_ID2, …, Pers_IDN$_1$) for a user (P1, P2, …, PN_1) thereby defining that the user is bound to the Authorized Domain (AD),

and/or in that

the means for binding at least one device (D1, D2, …, DM) to the domain identifier (Domain_ID) is adapted to:

obtain or generate a Domain Devices List (DDC) comprising the domain identifier (Domain_ID) and a unique identifier (Dev.ID1, Dev.ID2, …, Dev.IDM) for a device (D1, D2, …, DM) thereby defining that the device is bound to the Authorized Domain (AD).

15.   A system according to claim 14, wherein the means for binding at least one content item (C1, C2, …, CN_2) to the Authorized Domain (AD) is adapted to:

bind a content item (C1, C2, …, CN_2) to a User Right (URC1, URC2, … $URCN_2$), where said User Right (URC1, URC2, … $URCN_2$) is bound to a user (P1, P2, …, PN_1) which is bound to the Authorized Domain (AD), and/or

bind a content item (C1, C2, …, CN_2) to a Device Right (DevRC), where said Device Right (DevRC) is bound to a device (D1, D2, …, DM) which is bound to the Authorized Domain (AD), and/or

bind a content item (C1, C2, …, CN_2) to a Domain Rights (DRC1, DRC2, … $DRCN_2$), where said Domain Rights (DRC1, DRC2, … $DRCN_2$) is bound to the Authorized Domain (AD).

16. (Cancelled)

17. A system according to claim 15, wherein the User Right (URC1, URC2, … $URCN_2$) or the Device Right (DevRC) or the Domain Rights (DRC) comprises rights data (Rghts Dat) representing which rights exists in relation to the at least one content item (C1, C2, …, CN_2)

bound to the User Right (URC1, URC2, ... URCN$_2$) or the Device Right (DevRC) or the

Domain Rights (DRC1, DRC2, ... DRCN$_2$).

18.   A system according to claim 12, wherein the system further comprises means for controlling

access to a given content item bound to the Authorized Domain (AD) by a given device being

operated by a given user, where the means is adapted to:

      check if the given user is bound to the same Authorized Domain (AD) as the given

      content item, or

      check if the given device is bound to the same Authorized Domain (AD) as the given

      content item,

      and allow access for the given user via the given device and/or other devices to the

content item if the given user is bound to the same Authorized Domain (AD),

      or allow access for the given user and/or other users via the given device to the content

item if the given device is part of the same Authorized Domain (AD).

19.   A system according to claim 14, wherein the system further comprises means for controlling

access to a given content item (C1, C2, ..., CN$_2$), being bound to the Authorized Domain (AD)

and having a unique content identifier (Cont_ID), by a given device being operated by a given

user, where the means is adapted to:

      check if the Domain Devices List (DDC) of the Authorized Domain (AD) comprises an

      identifier (Dev.ID) of the given device, thereby checking if the given device is bound to

      the same Authorized Domain (AD) as the content item, and/or

      check if the Domain User List (DUC) of the Authorized Domain (AD) comprises an

      identifier (Pers_ID) of the given user (P1, P2, ..., PN$_1$) thereby checking if the given user

      is bound to the same Authorized Domain (AD) as the content item,

      and allow access to the given content item (C1, C2, ..., CN$_2$) by the given device (D1,

      D2, ..., DM) for any user if the given device is bound to the same Authorized Domain

      (AD) as the content item being accessed, and/or

allow access to the given content item ($C1, C2, ..., CN_2$) by any device including the given device for the given user if the given user is bound to the same Authorized Domain (AD) as the content item being accessed.

20. A system according to claim 18, wherein the means for binding at least one content item ($C1, C2, ..., CN_2$) to the Authorized Domain (AD) is adapted to:

> bind a content item ($C1, C2, ..., CN_2$) to a User Right ($URC1, URC2, ... URCN_2$), where said User Right ($URC1, URC2, ... URCN_2$) is bound to a user ($P1, P2, ..., PN_1$) which is bound to the Authorized Domain (AD), and

wherein the means for controlling access of a given content item is further adapted to further:

> check that the User Right ($URC1, URC2, ... URCN_2$) for the given content item specifies that the given user ($P1, P2, ..., PN_1$) has a right to access the given content item ($C1, C2, ..., CN_2$) and only allowing access to the given content item ($C1, C2, ..., CN_2$) in the affirmative.

21. A system according to claim 12, wherein every content item is encrypted and that a content right (CR) is bound to each content item and to a User Right (URC) or a Device Right (DevRC) or a Domain Rights (DRC), and that the content right (CR) of a given content item comprises a decryption key for decrypting the given content item.

22. A system according to claim 15, wherein

> the Domain Users List (DUC) is implemented as or included in a Domain Users Certificate, and/or

> the Domain Devices List (DDC) is implemented as or included in a Domain Devices Certificate, and/or

> the User Right ($URC1, URC2, ..., URCN_2$) is implemented as or included in a User Right Certificate, and/or

> the Device Right (DevRC) is implemented as or included in a Device Right Certificate, and/or

the Domain Rights (DRC1, DRC2, ..., $DRCN_2$) is implemented as or included in a Domain Rights Certificate.

23.   A non-transitory computer readable medium having stored thereon instructions for causing one or more processing units to execute the method according to claim 1.

EVIDENCE APPENDIX

No evidence has been submitted.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.